

# Authentication, Authorization and Accounting (AAA)

“AAA is an architectural framework for controlling a set of three independent security functions in a consistent manner.”, which indicates Authentication, Authorization & Accounting (AAA) combined together as an effective network and security management protocol.

The 3 As in the AAA framework provide the following services:

**Authentication:** It is defined as a mechanism to identify the user as who they are or who they are claiming before granting access to resources (Computer, network, network services, devices, etc.) There are a number of authentication types defined based on 3 categories:

- Something you have (such as cell phone).
- Something you are (such as fingerprint, iris recognition, face recognition).
- Something you know (such as password).

Some of the authentication types are named below:

- Static passwords -They do not change frequently unless it expires or the user changes it.
- One-time-Passwords – They are used to confirm your personal credentials like ATM pin through email or SMS.
- Digital Certificates – Such as X.509 to verify client and server identities and initiate secure SSL connections.
- Biometrics Credential – Using Face Recognition, Fingerprints, etc. to identify user identity.

**Authorization:** It is defined as a process of providing access to resources based on the access rights of users. When the user has completed the authentication process successfully, it is then provided access to the right kind of sources or services he/she must have access to and restrict access to what he/she cannot have access to. For example, an employee who has newly join an organization, can authenticate himself into the company employee system but has access to only the required resources and will be denied access to other than them.

**Accounting:** The Final ‘A’ of AAA has the purpose of sending and receiving critical server information like identity data usage, start and stop times. Moreover, used for auditing and reporting purposes. Accounting is used for logging information, tracking users, performing forensic investigation, detecting suspicious behavior, etc.

AAA’s functionality is utilized in Identity and Network Access Management. AAA uses protocols RADIUS ((Remote Authentication Dial-in User Service)) and TACACS+ (Terminal Access Controller Access-Control System) to authenticates the user to a network, that is from client to AAA server in a secure way.

## RADIUS and TACACS+

A RADIUS or TACACS server resides on a remote system and responds to queries from clients such as VPN clients, wireless access points, routers, and switches. The server then authenticates username/password combinations (authentication), determines whether users are allowed to connect to the client (authorization), and logs the connection (accounting).

TACACS+ is a client-server AAA protocol and offers many of the same AAA services as RADIUS.

## Directory Services with Active Directory

Active Directory is a technology created by Microsoft that provides a variety of network services, including the following:

- Lightweight Directory Access Protocol (LDAP)
- Kerberos-based and single sign-on (SSO) authentication
- DNS-based naming and other network information
- A central location for network administration and delegation of authority

Single sign-on (SSO) allows you to log on once and access multiple related but independent software systems without having to log in again. As you log on with Windows using Active Directory, you are assigned a token, which can then be used to sign on to other systems automatically.

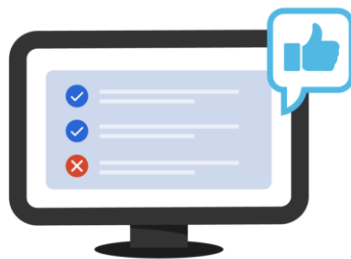
Finally, Active Directory allows you to organize all of your network resources—including users, groups, printers, computers, and other objects—so that you can assign passwords, permissions, rights, and so on to the identity that needs it. You can also assign who is permitted to manage a group of objects.

### Authentication



Confirms users are who they say they are.

### Authorization



Gives users permission to access a resource.

## Features

- Enhances the security and manageability of Enterprise & Government networks
- Deliver scalable Authentication control
- Robust Access Policy management
- Centralized Configuration management with the performance needed to tackle tens of thousands of concurrent users
- Market Leader in AAA/RADIUS/TACACS+ server for mid-sized to very Large Enterprises
- Unparallel support
- Quality Delivery

### Manage the risks associated with employee access

- 1 Authenticate**  
 Confirm the right person is accessing the system 
- 2 Authorize**  
 Give minimum access for their needs 
- 3 Accounting**  
 Monitor activities for security and compliance 

## FOR MORE INFORMATION

### About TechBridge

TechBridge is the World's leading Product & Solutions Company. Data Center Applications, Collaboration and Real Time Communication. DC Management and Monitoring, Disaster Management, Security, Collaboration and Cloud. Its market-leading Network Modernization, Unified Communications, Mobility and Embedded Communications solutions enable customers to quickly capitalize on growing market segments and introduce differentiating products, applications and services. We are an expert and leader in Government Solutions, Smart City Solutions, Data Centers and Large Enterprises. We do custom applications also, as per the customer requirements.

### Certificates:-

ISO 9001



ISO 27001



ISO 20000



CMMi L3



ISO 15408-1



PinkVERIFY



Mail us at: [sales@tech-bridge.biz](mailto:sales@tech-bridge.biz)

Address:- TechBridge Consultancy Services LLP

326, Tower B3, Spaze iTech Park, Sector-49, Sohna Road, Gurgaon-122018, Haryana